RECEIVED
CENTRAL FAX CENTER
SEP 05 2006

REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application is anticipated under the provisions of 35 U.S.C. § 102 or made obvious under the provisions of 35 U.S.C. § 103. Thus, the Applicants believe that all of these claims are in allowable form.

In addition, the Applicants' representative would like to thank Examiner Lemma for kindly taking a substantial amount of time on August 23, 2006 to discuss the merits of the subject invention. The Applicants' representative is aware of the time constraint that is placed on the Examiner and is appreciative of the Examiner's willingness to devote such large quantity of time to discuss the case on the merits.

I. REJECTION OF CLAIMS 1, 13, 16 AND 18 UNDER 35 U.S.C. § 112

Claims 1, 13, 16 and 18 stand rejected under 35 U.S.C. § 112, first paragraph, for allegedly failing to comply with the written description requirement. Specifically, the Examiner objects to the limitation wherein data is recited as being recoverable from an encrypted message "using only knowledge possessed by the recipient node prior to receipt of the encrypted message".

Although the Applicants disagree with the Examiner's position, the Applicants have nevertheless amended claims 1, 13, 16 and 18 to remove the disputed limitation. Accordingly, the Applicants respectfully request that the rejection of claims 1, 13, 16 and 18 under 35 U.S.C. § 112 be withdrawn.

II. REJECTION OF CLAIMS 1, 12-14 AND 16-18 UNDER 35 U.S.C. § 102

Claims 1, 12-14 and 16-18 stand rejected as being anticipated by the Aura patent (United States Patent No. 6,711,400, issued March 23, 2004, hereinafter "Aura"). In response, the Applicants have amended independent claims 1, 13, 16 and 18, from which claims 12, 14 and 17 depend, in order to more clearly recite aspects of the present invention.

Particularly, the Examiner's attention is directed to the fact that Aura fails to disclose or suggest the novel invention of decrypting an encrypted message in order to

recover data including an expected nonce value and a new nonce value, as claimed in Applicants' amended independent claim 1, 13, 16 and 18.

In contrast, Aura teaches that a recipient of a message (*i.e.*, a mobile station) enters data received from a sender (*i.e.*, an authentication center) into a one way hash function. If the result of the hash function matches a value sent by the sender, then the recipient has successfully authenticated itself to the network including the sender. Thus, there is no decryption being performed by the message recipient. That is, the recipient cannot "reverse" the received message (*e.g.*, using an encryption key shared with the sender) in order to retrieve content therefrom, but rather compares the result of an irreversible one-way hash function to a given value in order to determine if they match.

Notably, the Applicants' invention positively claims the novel method of decrypting an encrypted message in order to recover data including an expected nonce value and a new nonce value, as recited in Applicants' independent claims 1, 13, 16 and 18. Specifically, Applicants' independent claims 1, 13, 16 and 18 recite:

> 1. A secure method of transmitting a message between a sender node and a recipient node within a network collaboration group, the sender node and the recipient node sharing a secret encryption key and an expected nonce value comprising:
> generating a new nonce value known to the sender node;
> encrypting the message, the expected nonce value and the new nonce value, using the encryption key, to create an encrypted message; and
> transmitting the encrypted message from the sender node to the recipient node;
> wherein the encrypted message may be verified by the recipient node by decrypting the encrypted message and confirming that the encrypted message includes the expected nonce value. (Emphasis added)

> 13. A system for managing communications within a network collaboration group, comprising:
> means for generating a new nonce value;
> means for incorporating a message, an expected nonce value and

the new nonce value in an encrypted message;

means for transmitting the encrypted message from a sender node of the group to a recipient node of the group; and

means for verifying, by the recipient node, that the encrypted message includes the expected nonce value, wherein the expected nonce value is recoverable by decrypting the encrypted message. (Emphasis added)

16. A data-carrying signal for transmitting information securely between a master node and a member node of a network collaboration group, the signal being encrypted using an encryption key shared by the master node and the member node, the signal comprising:

the information to be transmitted;

an expected nonce value known to the master node and the member node; and

a new nonce value, different than the expected nonce, provided by a sender of the signal, the sender being one of the master node and the member node, where the expected nonce value and the new nonce value are recoverable from the signal by decrypting the signal. (Emphasis added)

18. A method for transmitting secure messages between a master node and a member node of a network collaboration group comprising:

encrypting messages encrypting messages using a key shared by the master node and the member node, so as to protect confidentiality of the message; and

embedding a plurality of updated nonce values within said encrypted messages so as to provide verifiable integrity, authenticity, and freshness for each of said messages, where said plurality of updated nonce values are recoverable from the messages by decrypting the messages. (Emphasis added)

The Applicants' invention is directed to methods and protocols for intrusion-tolerant management of collaborative network groups. As global users continue their migration to online network environments, the problem of vulnerability to malicious attacks (*e.g.*, by unauthorized users or "hackers") becomes more severe. Correspondingly, the need for "private" online groups that are resistant to intrusion by unauthorized users increases. Many known methods for providing private, secure

communication channels for authorized users (such as virtual private networks or VPNs) remain vulnerable to unauthorized intrusions such as replay attacks (illegitimate interception, copying and re-transmission of legitimate, encrypted traffic). To preserve system integrity and availability, it is important that such attacks be recognized as illegitimate communications.

The Applicants' invention provides a means for transmitting a message from sender to recipient in an intrusion-tolerant manner. Communications between sender and recipient are encrypted with a cryptographic key known by both parties and include two nonce values in addition to the message. The first nonce value is an expected nonce value, already known to the receiver, while the second nonce value is a new nonce value generated by the sender. When the receiver receives the encrypted message, the receiver verifies that the message includes the expected nonce value by decrypting the message using the cryptographic key. The presence of the expected nonce value confirms that the message is a legitimate message from the sender and is not part of an attack by an unauthorized party. The new nonce value then becomes the expected nonce value for a subsequent message (*e.g.*, from receiver to sender).

As discussed above, Aura fails to teach or suggest a method in which an encrypted message is decrypted in order to recover data including an expected nonce value and a new nonce value, as claimed in Applicants' independent claims 1, 13, 16 and 18. Therefore, the Applicants submit that independent claims 1, 13, 16 and 18 fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

Dependent claims 12, 14 and 17 depend from claims 1, 13 and 16 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 12, 14 and 17 are not anticipated by the teachings of Aura. Therefore, the Applicants submit that dependent claims 12, 14 and 17 also fully satisfy the requirements of 35 U.S.C. §102 and are patentable thereunder.

III. REJECTION OF CLAIMS 2-11 AND 15 UNDER 35 U.S.C. § 103

Claims 2-11 and 15 stand rejected as being made obvious by Aura in view of the Janson et al. patent (United States Patent No. 5,729,608, issued March 17, 1998,

hereinafter "Janson"). In response, the Applicants have amended independent claims 1, 13, 16 and 18, from which claims 2-11 and 15 depend, as discussed above in order to more clearly recite aspects of the present invention.

The Examiner's attention is directed to the fact that Janson, like Aura, fails to disclose or suggest the novel method of decrypting an encrypted message in order to recover data including an expected nonce value and a new nonce value, as positively claimed by the Applicants. Janson thus fails to bridge the gap in the teachings of Aura. Therefore, the Applicants respectfully submit that independent claims 1 and 13 fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

Dependent claims 2-11 and 15 depend, respectively, from claims 1 and 13 and recite additional features therefore. As such, and for at least the same reasons set forth above, the Applicants submit that claims 2-11 and 15 are not made obvious by the teachings of Aura in view of Janson. Therefore, the Applicants submit that dependent claims 2-11 and 15 also fully satisfy the requirements of 35 U.S.C. §103 and are patentable thereunder.

IV. CONCLUSION

Thus, the Applicants submit that all of the presented claims fully satisfy the requirements of 35 U.S.C. §102 and 35 U.S.C. §103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

9/5/06
Date

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702